Flash Point Paper

Security

Maintaining Continuous Compliance with GDPR

If you're like many people who suffer from compliance fatigue, you likely envision notebooks full of policies, costly expenditures to enforce them all, and auditors breathing down your neck waiting to point out your flaws.

When You Think of the Term Continuous Compliance, What Do You Picture in Your Mind?

In many ways, compliance does indeed create bureaucracy—work that you don't have time for. However, it doesn't have to be difficult, or costly, or overwhelming. Looking at compliance in the context of the EU's General Data Protection Regulation (GDPR), which impacts businesses around the globe, ongoing compliance requirements can be met and security improvements can be achieved if you go about it in the right ways.

In the context of identity governance and administration, how do you go about establishing and maintaining long-term continuous compliance with something as overwhelming as GDPR? Burying your head in the sand and hoping that nothing will ever come of it isn't a good strategy. Simply tweaking your written policies to make it look like things are getting done might serve to appease executives and auditors over the short term. But, again, it's no strategy. You need to step back and look at the bigger picture of how security technologies and processes can be adjusted to fulfill GDPR's specific requirements and how that might fit into your current program. Below are what I believe to be some key areas to evaluate and evolve:

You must determine what information is where along with who has access. This area of security alone accounts for a large portion of security risks in most organizations. You cannot secure the things that you don't acknowledge—or know about. The location of EU users and their data defines much of GDPR's security requirements. You must first know your network and your information flows before you can properly address the specific security needs around your network identities.

Ongoing GDPR compliance oversight requires the ability to solidify and secure the processes associated with people changing roles or leaving the organization altogether. A simple checklist or manual process is kludgy at best and can permit access to critical systems that can go undetected for months or even years. These are gaps that you likely cannot afford to take on and can prove to be indefensible when a confirmed breach occurs.

Ensure that GDPR compliance is not addressed in a vacuum. Siloed security controls that address each regulation separately often create more challenges—and liabilities—than they solve. Integrate your GDPR-focused identity governance efforts with other compliance

Is Your Organization Prepared to Maintain Compliance with the General Data Protection Regulation (GDPR)?

Here are some questions to ask yourself in order to determine if you are ready:

- *Do you have policies in place to monitor what information is affected, where it is stored and who has access to it?*
- *How do you manage role changes in order to ensure your users don't have more access than they require?*
- *Do the leaders of your various security and data management solutions communicate and coordinate efforts with each other?*
- *Does your organization conduct regular security assessments either internally or via an external partner?*

requirements where possible. This will likely involve complementary technologies such as security information and event management (SIEM), multifactor authentication, and data-centric controls such as data loss prevention (DLP) and cloud access security broker (CASB). The important thing is to not duplicate your efforts just in the name of GDPR. That is something that I see happening in many organizations. It not only creates distractions, but it serves as a time, energy, and money sap that's unnecessary in most situations. An ideal technical solution for identity governance would have the flexibility to address specific compliance needs and scale along with your higher-level IT and security initiatives. And it would do this with little to no architectural or procedural changes.

Don't forget about privileged account management. This is an often-overlooked layer of identity management which, when improperly implemented, not only introduces security risks and incidents that can go undetected, it can also impede day-to-day system administration. As with end users, system administrators need help streamlining their efforts and minimizing hassles associated with day-to-day tasks. The time and effort spent by these professionals is better served dealing with more strategic areas rather than getting distracted and out in the weeds dealing with unnecessary tactics.

Ongoing security audits and assessments are essential—not only for the sake of compliance but to ensure that your identity-related security policies and approaches are working. A critical look—using both internal tools and via the expertise of an outside party—is necessary to see where identity management gaps exist and can be (or have been) exploited for ill-gotten gains.

Proper IT and security governance requires reasonable controls, ongoing maintenance in the form of monitoring and tweaking, and prompt remediation when necessary. It's all about determining risk, addressing those risks, and closing the gaps to keep everything in check and everyone happy.

Compliance doesn't have to be a bad word. If you want to meet GDPR's requirements and, at the same time, improve your overall security program, it's all about taking a common-sense approach. Looking at holistic security requires everything from network monitoring to software patching to ongoing security evaluations. Fleshing things out with physical security, policy management, and contingency planning will bring your security controls full-circle. This will allow your organization to not only meet but exceed whichever compliance requirements come your way.

Given all the parties involved—from the service desk to compliance to HR and legal—when IT and security management systems are fine-tuned, it can improve the overall user experience. A streamlined approach to identity governance can be a valuable tool for supporting security efforts over the long haul—something I often see clients struggling with when tangible business benefits are not perceived or fully actualized.

IT and business involve change and adapting to that change. The important things are to acknowledge your security challenges, vow to close the gaps, and stay involved over the long-term. GDPR compliance is not a one-time checkbox like many people have treated other regulations such as HIPAA and GLBA. Rather, it's a philosophy that requires both the willingness to do what's right and the discipline to see it through. A simple way to fall out of compliance with GDPR is to become complacent with where you're at. It's easy to get distracted but don't be tempted by that path. Instead, treat information security as a process rather than a goal and reasonable compliance (GDPR and otherwise) will come about as a result.

About the Author

Kevin Beaver is an independent information security consultant, writer, professional speaker, and expert witness with Atlanta-based Principle Logic, LLC. With three decades of experience in the industry, Kevin performs independent security assessments and consulting work to help businesses uncheck the boxes that keep creating a false sense of security. He has authored/co-authored 12 books on information security including the best-selling Hacking For Dummies and The Practical Guide to HIPAA Privacy and Security Compliance. Kevin can be reached at **www.principlelogic.com** and you can follow in on Twitter at **@kevinbeaver**.

Contact us at:
www.microfocus.com

About Micro Focus

Micro Focus® delivers identity-centric security that reduces risk, improves experience, drives innovation and increases business value to organizations all over the world.

Regulations concerning privacy and separation-of-duty requirements create a lot of overhead for your organization. You need to know whether you are compliant to IT regulations or mandates related to identity and access, and can pass an audit.

We can help you:

- Use policies to ensure that IT regulations are not violated.
- Monitor user activity and enforce IT regulatory compliance.
- Maintain the integrity of your access policies.
- Demonstrate access governance and IT regulatory compliance.
- Combat access elevation and entitlement creep.

To learn more about how we can help, please visit our Identity and Access Governance page at **www.netiq.com/governance**.

184-000009-001 | M | 05/18 | © 2018 Micro Focus. All rights reserved. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.